Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 1999 Proceedings

Americas Conference on Information Systems (AMCIS)

December 1999

When Managers Make Irrational Contingency Planning Decisions

Stephen Lunce
Texas A&M International University

When Managers Make Irrational Contingency Planning Decisions

Stephen E. Lunce, Texas A&M International University, slunce@tamiu.edu

Abstract

Organizations depend upon their strategic systems for both survival and success in the competitive environments of today. In this environment exist threats to the security of these vital systems; these include, but are not limited to: natural disasters (e.g. floods and hurricanes), sabotage (e.g., hackers and disgruntled employees), and human error (e.g. the "Y2K bug"). This paper reviews some relevant management issues involved in the recognition of the existence of a threat and the reactions that organizations can take in response to this recognition.

Introduction

In the information age, systems have become increasingly important to the survival and success of organizations as they become more reliant upon information as both a product and source of intelligence about the environment in which they exist. The environment is not benign, and as many researchers have demonstrated, threats from the environment continue to place information systems at risk (Aasgaard, et al, Christensen and Schkade, Lunce, and Subhani). When these threats are actualized as hazards the security of the information system is likely to be compromised.

Organizational success is relative to the consequences of the decisions made by the managers within the organization. It has been stated that "all managerial activities revolve around decision making. The manager is first and foremost a decision maker" (Turban, p. 4). The decision maker must be aware that a threat to the security of the organization's information system exists in the environment. However, awareness alone is not a sufficient motivation for action for most decision makers. In a threatening situation there are some general principles which may be applied; these principles are: threat evaluation, response identification, and cost benefit determination (Christensen and Schkade).

The Irrational Decision

A manager who is aware of the threat has developed a perceptual awareness. With this perception, the decision maker can begin to execute the managerial responsibilities of protecting and preserving the organizations assets. If the threat has been identified and the manager determines that a significant threat exists, the action must be taken to protect the system that is at risk. Failure to take protective action will either violate legislative requirements, such as the Foreign Corrupt Practices Act, or will provide evidence that the decision maker does not regard the threat as serious enough to merit preemptive action.

The premise that threats exist for systems in general is universally accepted, and these threats to the security of systems have been demonstrated to be isomorphic across systems (Christensen). The issue that this acceptance presents is, if threats are real, and if threats are perceived by decision makers, how does this perception effect the way in which decision makers go about their decision making process in relation to the potential development of disaster recovery plans. How the organization responds to these threats is a reflection of the decision maker's perception of the significance of the threat. If the decision maker perceives a serious risk, one that if incurred would result in significant damage to the organization, some action will be initiated by the perception. There will be evidence of this perception in a specific subset of the security measures implemented by the organization. That subset is the organization's contingency plan (Lunce).

Systems, including business systems, exist in a causal environment. The activities of nature impact nature itself and the artificial systems that reside within the natural environment. Everything that is exist in some way a result of some precedent cause. The causes exist *a priori* and their existence is evidenced by their results. These causes might be described as action motivators, i.e. through their existence or occurrence, a resultant action is taken or a new state of being is achieved. Similarly, in the business world, situations are the result of *a priori* causes. Some of those causes may result in damage or harm to the organization. If an antecedent event may damage an organization, it can properly be referred to as a threat. The creation of source code that is unable to adequately manipulate dates greater than 1999 is an example of an *a priori* cause that resulted in a serious threat to organizational survival, i.e., the *Y2K bug*. A rational manager will always seek to maximize profitability, or to minimize costs; the actualization of an unmitigated risk would be evidence of an irrational decision.

Threats might appear in one of two forms. They will either be natural events that might impact the organization, or they will be the result of some human activity. For example, storms such as hurricanes and tornadoes would be included in the category of natural threats. Deliberate or accidental destruction or corruption of a database would be

considered within the category of the man made threats. The Y2K problem falls into this later category, and it resulted from a supposedly rational *a priori* decision to save space in computer storage devices.

If threats do exist, why do organizations at the direction of their management team respond differently to the existence of events that might damage that organization? The answer seems to reside within the perceptions and risk acceptance behaviors of the managers responsible for organizations. The severity of the threat, and the probability of its occurrence with detrimental impact upon the organization is a perceptual idea that will vary from decision maker to decision maker. This variance in perception is analogous to two individuals observing the same art work, and one of the individuals appreciating the work while the other is not impressed. Decision makers' views or perceptions of the significance of the threat, i.e. the amount of risk to which the organization is exposed, varies from individual to individual. Humans will look at the same situation, regardless of its nature, and the perspectives will vary from individual to individual. The model reflects this variability.

If a decision maker perceives within a situation a large enough risk, the decision maker will take steps to mitigate the risk. For example, if the risk is fire (a causality loss that may occur), the decision maker may purchase an insurance policy in order to protect the property from potential loss. Acquiring causality insurance is common in many areas of resource management. However, information systems are a relatively new component in the organizational structure. Their importance as a resource has been established, but the method best suited to placing a dollar value on these resources are still being debated. Without a concrete starting point, it is difficult for management to justify expenditures for the insurance protection of a resource, unless the potential threats can be mentally justified as actually serious and significant. This justification is based upon the decision maker's perception of the severity of the risk. The greater the perceived severity, the more likely the decision maker is to take action to preserve the resource that is at risk, assuming that the value of the resource has been established.

A Case Study of a Successful Plan

First Interstate Bank is an international financial institution. "At 10:30 p.m. the night of May 4, 1988, Los Angeles' worst high-rise fire swept through the 62 story downtown headquarters of First Interstate Bank destroying floors 12 through 16" (Coleman, p. 5). Forty percent of the fire companies of Los Angeles responded to the fire. The fire was suppressed by 3:00 a.m. 5 May, a normal work day in the banking industry.

The risk, or that event that caused the damage, was a fire. Risks are threats that have been actualized (i.e. they result in losses, which may be either physical or financial or a combination of both). The threat in this case was never publicly identified; however, a faulty electrical system has been suspected. The effects of the this disaster were widespread. The Securities Trading Department, located on the twelfth floor, was totally destroyed. This department typically processed three to five billion ($3,000,000,000 - $5,000,000,000) in transactions every day. Temperatures in the fire exceeded 2,000^{o} Fahrenheit; the mini and micro computers in the bond trading department failed to withstand the heat. Although the fire was contained above the twelfth floor, the eleventh floor, which contained First Interstate's security vault and its paper archives, was totally destroyed by water from the fire containment efforts. Not only were major data processing facilities destroyed, approximately 2,000 employees were displaced.

The management of First Interstate Bank was mandated to have a contingency plan in place by regulations such as Banking Circular BC-177; however, they were committed to insuring that their plan was both current, well tested, and functional. At 11:00 p.m. bank management declared an emergency which activated the contingency plan. The emergency operations center (E.O.C.) was activated. The E.O.C. is a remote site that had been equipped with computers, software, and archival data that would allow the bank to quickly recover critical (but not all) functions. Within twenty-four (24) hours all key units were functional, although some of the traders had to utilize portable lap-top computers and access the bank's files via modems. To the external environment serviced by First Interstate, the next day (May 5th) appeared to be business as usual, even though banking could not take place in the Bank's high-rise building. The main branch reopened two days after the fire in leased offices. With A.T.& T.'s help, phone service was restored to some 3,000 phone numbers by the morning of 7 May, only seventy-two hours after the fire. The disaster had virtually no effect on the 1988 profitability of the bank.

Strategic Implications of Contingency Plans

Information has value to organizations in both strategic planning and tactical operations (Frenzel). That valuable information is provided by the organization's information systems. Threats exist in the environment wherein the organization resides. If these threats are actualized, the system which provides information may be damaged or destroyed. If the existence of the threats is recognized, and if any threat is perceived as large enough to adversely effect the operations of the organization, then the rational decision maker who perceives the threat will be motivated to take action to protect the information providing resource. The first action is the development of a plan to deal with the threat should it occur. This is a contingency plan, and this plan comes into existence as a direct result of a decision

maker's perception of a potential loss, and as insurance against that potential loss.

Threats to Information Systems: A Risk Matrix

IMPACT ON THE FIRM				
Mission Failure				—
Business Interruption			—	
Business Disruption		—		
Little or None	—			
Duration of Outage	**Moment**	**< 48 Hrs.**	**2-14 Days**	**> 14 Days**

Figure 1: A Risk Matrix (after Toigo)

The perceived size of the potential loss is reflected in the sophistication of the contingency plan and the quality of the exercise of the plan, as the model illustrates. The greater the possible loss, the more sophisticated will be the steps taken by the rational decision maker to insure that if the threat is actualized, the damage has been mitigated. The more of the plan that can be practiced the more employee familiarity will be developed. As familiarity increases, the possibility of unforeseen occurrences in the actual execution of the plan will decrease. A plan that is very sophisticated may not be as effective a recovery tool as a less sophisticated plan that has been well rehearsed. If personnel know how to respond and know precisely who is responsible for which activities, the recovery window will be reduced. This reduction may mean the difference in survival of the organization at a level that resembles the pre-actualization of the threat, and the failure of the organization to survive for an extended period of time in the post-incident environment (Christensen and Schkade).

It has been demonstrated that the existence of the contingency plan is a function of the perception of rational decision makers (Lunce), but several other issues must be addressed. Prior research has indicated that the determining factor in the cash outlay for the development of a contingency plan is the time criticality of recovery. If the time between failure and recovery is insignificant, then the amounts budgeted to recovery plans should be expected to be less than if the time to recovery is critical to the functionality of the organization (Subhani). If perception is the motivator, and if time is the critical dimension, then the awareness of the existence of a previously unperceived threat should motivate decision makers toward either creation of new plans or exercise and possible revision of existing plans. Unfortunately, not all decision makers choose to the respond to there perceptions of the existence of real threats to the organization.

Concluding Remarks

Organizations could be categorized along several dimensions in order to better understand the nature of their contingency planning. This understanding could provide insights into how decision makers think and how they actually perceive the existence of real threats within the environment. These insights may help future decision makers increase the effectiveness with which they are able to manage their information resources. Analysis of the insights gained may demonstrate a need to devote time and effort to a specific class of planning aids to support decision makers who have perceived that a significant risk exists and have decided to act upon that perception.

References

Aasgaard, D.O., Cheun, P.R., Hulbert, B.J., and Simpson, M.C., "An Evaluation of Data Processing 'Machine Room' Loss and Selected Recovery Strategies (WP-79-04)", Minneapolis: University of Minnesota, Management Information Systems Research Center, 1978.

Christensen, S. R. and Schkade, L. L., "Financial and Functional Impacts of Computer Outages on Business", (CRIS-87-01), Center for Research on Information Systems, University of Texas at Arlington, 1987.

Coleman, P., "The First Interstate Bank Fire," *Disaster Recovery Journal*, 1(4), Oct., 1988, pp. 5-8.

Frenzel, C.W., *Management of Information Technology*, Course Technology, Cambridge, MA, 1999.

Lunce, S.E., "An Investigation of Managerial Issues Involved in Contingency Planning for Information Systems", Ph.D. Dissertation, UTA, December, 1994.

Subhani, S., "Decision Model for Optimal Selection of Recovery Plans for Computer Outages", Ph.D. Dissertation, University of Texas at Arlington, December, 1989.

Turban, E. and Aronson, J.E., *Decision Support Systems and Intelligent Systems*, Prentice-Hall, Englewood Cliffs, NJ, 1998.